ZFW

AF

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	09/822,539
Filing Date	March 30, 2001
First Named Inventor	Priya Govindarajan
Art Unit	2182
Examiner Name	Casiano, A.
Total Number of Pages in This Submission: 20	Attorney Docket Number: 42390P10459

ENCLOSURES *(check all that apply)*

- [X] Fee Transmittal Form
  - [X] Fee Attached
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
  - [ ] PTO/SB/08
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Basic Filing Fee
  - [ ] Declaration/POA
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [X] Appeal Communication to Group **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [X] Other Enclosure(s) *(please identify below):*

Check No. _____ in the amt of $500.00.

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Gordon R. Lindeen III, Reg. No. 33,192 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	July 6, 2005

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	**Debbie Casias**		
Signature	Debbie Casias	Date	**July 6, 2005**

Based on PTO/SB/21 (04-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 06/04/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT	($)	500.00

Complete if Known	
Application Number	09/822,539
Filing Date	March 30, 2001
First Named Inventor	Priya Govindarajan
Examiner Name	Casiano, A.
Art Unit	2182
Attorney Docket No.	42390P10459

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below
☐ Charge fee(s) indicated below, except for the filing fee
☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.
☒ Credit any overpayments

FEE CALCULATION

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500.00
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) _____

SUBTOTAL (2) ($) 500.00

SUBMITTED BY Complete (if applicable)

Name (Print/Type)	Gordon R. Lindeen III	Registration No. (Attorney/Agent)	33,192	Telephone	(303) 740-1980
Signature				Date	07/06/05

Based on PTO/SB/17 (12-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 12/15/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☒ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.*

FACSIMILE

☐ *transmitted by facsimile to 703-872-9306 at the U.S. Patent and Trademark Office.*

Date: July 6, 2005

Debbie Casias 7/6/05

Debbie Casias ***Date***

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Patent Application of:		
	Priya Govindarajan et al.	
Serial No.:	09/822,539	Art Unit: 2182
Filed:	3/30/2001	
		Examiner: Angel L. Cassiano
For:	Method and Apparatus for Discovering Network Topology	

07/11/2005 MWOLDGE1 00000028 09822539
01 FC:1402 500.00 OP

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313

APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Applicants (hereafter "Appellants") hereby submit this Brief in triplicate in support of its appeal from a final decision by the Examiner, mailed February 9, 2005 in the above-captioned case. Appellants respectfully request consideration of this appeal by the Board of Patent Appeals and Interferences for allowance of the above-captioned patent application.

An oral hearing is not desired.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052-8119.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

III. STATUS OF THE CLAIMS

Claims 1-22 are currently pending in the above-referenced application. Claims 1-22 were rejected in the Final Office Action mailed February 9, 2004, and are the subject of this appeal.

Claims 1-22 stand rejected under 35 U.S.C. § 103.

IV. STATUS OF AMENDMENTS

In response to the Final Office Action mailed on February 9, 2005, rejecting claims 1-22, Appellants timely filed a Notice of Appeal on May 6, 2005.

A copy of all claims on appeal is attached hereto as Appendix A.

V. SUMMARY OF THE INVENTION

Any networked domain will typically have a number of devices responsible for routing the traffic around the network. In order to survive a failure of any one device or link, a network is typically designed with redundant back-up routes. Some networks can have multiple interconnected back-up routes. Over time, devices can be moved, added, removed or replaced, routes can be moved or altered and device configurations can be changed. As a result, any documentation of the original network design, if it was created, becomes outdated. When problems occur, troubleshooting is made more difficult without accurate information on the network's topology. When new demands are to be applied to the network, it may not be possible to determine how to reconfigure the network without knowledge of the network's existing topology. When performance is to be measured or improved, it is difficult to determine how to develop the network without understanding all of the links and which devices are connected to each one. *See Background of the Invention, page 2, paragraph 2.*

The present invention can be implemented by using PING and Traceroute at sources distributed throughout a network and then piecing all of the collected information together to determine the overall topology of the network. The PING and Traceroute sources will be called Smartlinks. They respond to policies sent to them from a designated central server. In brief, the Smartlinks register themselves to the server and the server then sends policies to each of the Smartlinks. The Smartlinks execute the policies by running Traceroutes to each other. This allows them to identify all of the hosts that are between each Smartlink. This information is then sent to the central policy server which compiles the reports from each Smartlink to determine the topology of all of the network that is within the Smartlinks. The server can then render the topology in the form of lists, charts, graphs or a database. *See Detailed Description of the Invention, page 6, paragraph 6.*

The elements of Claim 1 are provided below with references to the example structures and operations provided by embodiments shown in the drawing figures. The references to the Detailed Description can be found quickly by reference to the drawing figures.

registering (Figure 2, 44) a first network device (Figure 1: SL1, (Smartlink 1), Figure 2: 42) and a second network device (Figure 1, SL2, (Smartlink 2)) to a policy server (Figure 2: 40);

receiving (46) network discovery policies from the policy server at the first and second network devices (SL1, SL2);

identifying (48) the second network device (SL2) at the a first network device (SL1) in accordance with the received policies;

sending (48, run traceroute) a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies;

(50, 52, 54, 60) compiling the established identities to determine the topology of the network.

VI. ISSUES PRESENTED

Whether claims 1-22 are rendered obvious under 35 U.S.C. 103 based on references that fail to teach or suggest the claimed limitations of "receiving network discovery policies from the policy server" and "sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies.".

VII. GROUPING OF CLAIMS

For the purposes of this appeal, claims 1-22 stand or fall together.

VIII. ARGUMENT

REJECTION OF CLAIMS 1-22 UNDER 35 USC §103 IS IMPROPER BECAUSE THE REFERENCES DO NOT SHOW THE ELEMENTS OF THE CLAIMS WHETHER ALONE OR IN COMBINATION

The Examiner has rejected claims 1-4, 6-8, 10-12, 14-18 and 21-22 under 35 U.S.C. § 103(a) as being unpatentable over Nelson, U.S. Patent No. 5,835,720 ("Nelson") in view of Reichmeyer et al., U.S. Patent No. 6,286,038 ("Reichmeyer"). In Nelson, the network manager 40 builds its hierarchical data structure by first accessing its own IP address table and local routing table in its ARP cache. (Col. 5, line 39) The local routing table is used to identify a default router. (Col. 5, line 43). The NM then retrieves the routing table, IP address table and ARP table of the default router. (Col. 5, line 61). The network manager uses the retrieved routing table to find more routers and retrieve their tables until it has completed the construction of the hierarchical data structure. (Col. 6, lines 16-29). The network manager then pings all the addresses for verification.

The process outlined in Nelson is limited by the knowledge of the discovered routers. Routers are not generally designed to determine network topology but to deliver messages. In addition, because it relies on ping and traceroute type messages sent from the network manager 40, as described in columns 6 and 7, it suffers from the same disadvantages described in paragraphs 4 and 5 of the present application.

In the present invention as recited, for example, in Claim 1, as amended, there are three different entities at work: a policy server, a first network device, and a second network device. The policy server receives registrations and sends out network discovery policies to the first and the second network device, such as the Smartlinks described in the application. The first and second network devices then run the policies to discover the network. The identities established by running the policies is then used to determine

the topology. By using multiple devices that run specific policies, the shortcomings of Nelson may be overcome. As mentioned above, these shortcomings include the limits of using ping and traceroute from a single location and the limits inherent in routing tables that are developed for use in routing, not for network topology. Nelson does not teach or suggest "sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies"

The operation of Reichmeyer, is presented pretty clearly in Figure 3 on the face of the patent. The subdomain routers send neighbor info and pre-config. info to the central configuration server and the central configuration server sends the config. info which it has stored in a file. The many pages of the reference are directed to the details of how this is done. In all of this description, there are no policies sent which would allow for the element of "sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies" as recited in Claim 1. See, for example, Column 3, lines 47-52, discussing the transfer of the configuration information. See Column 4, lines 54-58, regarding the contents of the configuration info file.

Reichmeyer is not directed to automatically discovering the configuration of a network or "compiling the established identities to determine the topology of the network." Instead, Reichmeyer admits of the difficulties in doing so and allows the system administrator to create topology and set pre-configuration files manually. See Column 3, lines 20-29, Column 5, lines 8-10, Column 10, lines 35-43. In short, Reichmeyer has a network with a manually predetermined topology. When a subdomain router is added, it either has a pre-configuration file saying where it fits into the network or it uses neighbor discovery to allow the configuration server to figure out where it fits into the network. The network topology is not discovered automatically and it would not

be obvious to combine the two references to create a system that automatically discovers the network.

The Examiner writes that Reichmeyer shows "a policy server in communication with first and second network devices." The reference shows instead a configuration server in communication with first and second network devices (routers). The Examiner further writes that "identities are established by collecting information on the network devices." At Column 8, lines 22-42, a list of information that may be sent by a network device to the configuration server is provided. This includes various identification information.

The Examiner next writes that "in accordance to this protocol, the prior art method gathers information and determines the topology of the network." While the configuration server gathers information, there is no suggestion in the reference that the configuration server determines the network topology. Furthermore, the Examiner identifies the relevant part of Claim 1, to be "registering a first network device and a second network device to a policy server," and "receiving network discovery policies from the policy server at the first and second network devices." Applicants are unable to find any suggestion in the reference of the second element.

Accordingly, absent this teaching in the reference. The claims are believed to be allowable. The Examiner would seem to interpret Nelson as if it has the two network devices of Claim 1 and then ignore lack of a server in Nelson. The Examiner would then seem to supply a server from Reichmeyer, but this server does not do any of what the server of Claim 1 does. The fundamental operation as defined in the claims is ignored and accordingly the rejection is respectfully traversed.

In the Advisory Action of April 27, 2005, the Examiner defends the combination of the two references to reject the application. The Examiner acknowledges the lack of a policy server in Nelson and then suggests that it would be obvious to apply the policy

server from Reichmeyer. As noted above, the server in Reichmeyer does not do any of what the server of Claim 1 does.

Accordingly, neither reference teaches or suggests "receiving network discovery policies from the policy server" nor "sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies." The Examiner's rejection is therefore inappropriate and Appellant respectfully requests that it be reversed.

IX. CONCLUSION

Appellant respectfully submits that all the appealed claims in this application are patentable and requests that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

This brief is submitted in triplicate, along with a check for $500.00 to cover the appeal fee for one other than a small entity as specified in 37 C.F.R. § 1.17(c). Please charge any shortages and credit any overpayment to out Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: 7/6, 2005

Gordon R. Lindeen III
Attorney for Appellant
Registration Number: 33,192

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030
(303) 740-1980

APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(7))

1. A method comprising:

registering a first network device and a second network device to a policy server;

receiving network discovery policies from the policy server at the first and second network devices;

identifying the second network device at the first network device in accordance with the received policies;

sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies;

compiling the established identities to determine the topology of the network.

2. The method of Claim 1, wherein identifying the second network device comprises receiving an address of the second network device from a third network device.

3. The method of Claim 1, wherein the first network device comprises a plurality of network interfaces, the method further comprising selecting an interface to the second device by sending a packet from each of the plurality of network interfaces to an address of the second network device and selecting an interface that corresponds to any reply received from the second network device.

4. The method of Claim 3, wherein sending a packet from each of the plurality of network interfaces comprises sending a PING packet from each of the plurality of network interfaces.

5. The method of Claim 1, wherein sending the message comprises sending a plurality of messages to the second network device, each message having an incrementally greater time to live until a message reaches the second network device.

6. The method of Claim 1, wherein sending the message comprises executing a Traceroute utility at the first network device to determine the route of a packet between the first and second network device.

7. The method of Claim 1, further comprising:

identifying a third network device at the first network device;

sending a message from the first network device to the third network device, the message establishing the identity of any network device between the first network device and the third network device.

8. The method of Claim 1, further comprising sending a packet to a third network device to provoke the third network device to identify an address corresponding to a port at which the packet was received and wherein compiling further comprises compiling the identified address.

9. The method of Claim 1, further comprising sending a packet to a third network device addressed to a port that does not exist on the third network device in order to provoke the third network device to send an error message to the first network device that identifies an address of the third network device corresponding to the port at

which the packet was received and wherein compiling further comprises compiling the identified address.

10. A machine-readable medium having stored thereon data representing sequences of instructions which, when executed by a machine, cause the machine to perform operations comprising:

registering a first network device and a second network device to a policy server;

receiving network discovery policies from the policy server at the first and second network devices;

identifying the second network device at the first network device in accordance with the received policies;

sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies;

compiling the established identities to determine the topology of the network.

11. The medium of Claim 10, wherein the instructions for identifying the second network device further comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising receiving an address of the second network device from a third network device.

12. The medium of Claim 10, wherein the first network device comprises a plurality of network interfaces, the instructions further comprising instructions which, when executed by the machine, cause the machine to perform further operations comprising selecting an interface to the second device by sending a packet from each of

the plurality of network interfaces to an address of the second network device and selecting an interface that corresponds to any reply received from the second network device.

13. The medium of Claim 10, wherein the instructions for sending the message further comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising sending a plurality of messages to the second network device, each message having an incrementally greater time to live until a message reaches the second network device.

14. The medium of Claim 10, further comprising instructions, when executed by the machine, cause the machine to perform further operations comprising:

identifying a third network device at the first network device;

sending a message from the first network device to the third network device, the message establishing the identity of any network device between the first network device and the third network device.

15. The medium of Claim 10, further comprising instructions which, when executed by the machine, cause the machine to perform further operations comprising sending a packet to a third network device to provoke the third network device to identify an address corresponding to a port at which the packet was received and wherein the instructions for compiling comprise further instructions which, when executed by the machine, cause the machine to perform further operations comprising compiling the identified address.

16. A method comprising:

registering a first network device and a second network device to a policy server;

receiving network discovery policies from the policy server at the first and second network devices;

identifying the second network device at the first network device in accordance with the received policies;

sending a Traceroute message from the first network device to the second network device, to determine addresses of any network device between the first network device and the second network device in accordance with the received policies;

compiling the addresses to determine the topology of the network.

17. The method of Claim 16, wherein identifying the second network device comprises receiving an identification of the second network device, including its address from a policy server.

18. The method of Claim 16, wherein the first network device comprises a plurality of network interfaces, the method further comprising selecting an interface to the second device by sending a PING message from each of the plurality of network interfaces to an address of the second network device and selecting an interface that corresponds to any reply received to the PING message from the second network device.

19. The method of Claim 16, wherein the Traceroute message comprises a plurality of messages to the second network device, each message having an incrementally greater time to live until a message reaches the second network device.

20. The method of Claim 16, further comprising sending a packet to a third network device addressed to a port that does not exist on the third network device in

order to provoke the third network device to send an error message to the first network device that identifies an address of the third network device corresponding to the port at which the packet was received and wherein compiling further comprises compiling the identified address.

21. The method of Claim 1, further comprising sending the established identities to the policy server in accordance with the received policy.

22. The method of Claim 21 wherein compiling comprises compiling the established identities at the policy server to determine the topology of the network.

APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(7))

1. A method comprising:

registering a first network device and a second network device to a policy server;

receiving network discovery policies from the policy server at the first and second network devices;

identifying the second network device at the first network device in accordance with the received policies;

sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies;

compiling the established identities to determine the topology of the network.

2. The method of Claim 1, wherein identifying the second network device comprises receiving an address of the second network device from a third network device.

3. The method of Claim 1, wherein the first network device comprises a plurality of network interfaces, the method further comprising selecting an interface to the second device by sending a packet from each of the plurality of network interfaces to an address of the second network device and selecting an interface that corresponds to any reply received from the second network device.

4. The method of Claim 3, wherein sending a packet from each of the plurality of network interfaces comprises sending a PING packet from each of the plurality of network interfaces.

5. The method of Claim 1, wherein sending the message comprises sending a plurality of messages to the second network device, each message having an incrementally greater time to live until a message reaches the second network device.

6. The method of Claim 1, wherein sending the message comprises executing a Traceroute utility at the first network device to determine the route of a packet between the first and second network device.

7. The method of Claim 1, further comprising:

identifying a third network device at the first network device;

sending a message from the first network device to the third network device, the message establishing the identity of any network device between the first network device and the third network device.

8. The method of Claim 1, further comprising sending a packet to a third network device to provoke the third network device to identify an address corresponding to a port at which the packet was received and wherein compiling further comprises compiling the identified address.

9. The method of Claim 1, further comprising sending a packet to a third network device addressed to a port that does not exist on the third network device in order to provoke the third network device to send an error message to the first network device that identifies an address of the third network device corresponding to the port at

which the packet was received and wherein compiling further comprises compiling the identified address.

10. A machine-readable medium having stored thereon data representing sequences of instructions which, when executed by a machine, cause the machine to perform operations comprising:

registering a first network device and a second network device to a policy server;

receiving network discovery policies from the policy server at the first and second network devices;

identifying the second network device at the first network device in accordance with the received policies;

sending a message from the first network device to the second network device, the message establishing the identity of any network device between the first network device and the second network device in accordance with the received policies;

compiling the established identities to determine the topology of the network.

11. The medium of Claim 10, wherein the instructions for identifying the second network device further comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising receiving an address of the second network device from a third network device.

12. The medium of Claim 10, wherein the first network device comprises a plurality of network interfaces, the instructions further comprising instructions which, when executed by the machine, cause the machine to perform further operations comprising selecting an interface to the second device by sending a packet from each of

the plurality of network interfaces to an address of the second network device and selecting an interface that corresponds to any reply received from the second network device.

13. The medium of Claim 10, wherein the instructions for sending the message further comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising sending a plurality of messages to the second network device, each message having an incrementally greater time to live until a message reaches the second network device.

14. The medium of Claim 10, further comprising instructions, when executed by the machine, cause the machine to perform further operations comprising:

identifying a third network device at the first network device;

sending a message from the first network device to the third network device, the message establishing the identity of any network device between the first network device and the third network device.

15. The medium of Claim 10, further comprising instructions which, when executed by the machine, cause the machine to perform further operations comprising sending a packet to a third network device to provoke the third network device to identify an address corresponding to a port at which the packet was received and wherein the instructions for compiling comprise further instructions which, when executed by the machine, cause the machine to perform further operations comprising compiling the identified address.

16. A method comprising:

registering a first network device and a second network device to a policy server;

receiving network discovery policies from the policy server at the first and second network devices;

identifying the second network device at the first network device in accordance with the received policies;

sending a Traceroute message from the first network device to the second network device, to determine addresses of any network device between the first network device and the second network device in accordance with the received policies;

compiling the addresses to determine the topology of the network.

17. The method of Claim 16, wherein identifying the second network device comprises receiving an identification of the second network device, including its address from a policy server.

18. The method of Claim 16, wherein the first network device comprises a plurality of network interfaces, the method further comprising selecting an interface to the second device by sending a PING message from each of the plurality of network interfaces to an address of the second network device and selecting an interface that corresponds to any reply received to the PING message from the second network device.

19. The method of Claim 16, wherein the Traceroute message comprises a plurality of messages to the second network device, each message having an incrementally greater time to live until a message reaches the second network device.

20. The method of Claim 16, further comprising sending a packet to a third network device addressed to a port that does not exist on the third network device in

order to provoke the third network device to send an error message to the first network device that identifies an address of the third network device corresponding to the port at which the packet was received and wherein compiling further comprises compiling the identified address.

21. The method of Claim 1, further comprising sending the established identities to the policy server in accordance with the received policy.

22. The method of Claim 21 wherein compiling comprises compiling the established identities at the policy server to determine the topology of the network.